We claim:

1. A computerized method for key-based secure storage comprising:

downloading content and an access predicate that specifies requirements for an application to access the content;

obtaining a storage key;

encrypting the content using the storage key; and

associating the access predicate with the encrypted content.

2. The computerized method of claim 1, further comprising:

decrypting the content for access by an application only if the application meets the requirements specified in the access predicate.

3. The computerized method of claim 1, wherein the storage key is an application storage key and obtaining the application storage key comprises:

generating a seed value;

producing a hash seed value based on the seed value using a one-way hash function; and

generating the application storage key from the hash seed value.

4. The computerized method of claim 1, wherein the storage key is a user storage key and obtaining the user storage key comprises:

generating a seed value;

producing a first hash seed value based on the seed value using a one-way hash

function;

producing a second hash seed value based on the seed value and a user identifier using a keyed hash function; and

generating the user storage key from the second hash seed value.

5. The computerized method of claim 1, further comprising:

obtaining an operating system storage key; and

encrypting the access predicate with the operating system storage key.

6. The computerized method of claim 5, further comprising:

encrypting a plurality of other storage keys using the operating system storage key, wherein the other storage keys are selected from the group consisting of application storage keys and user storage keys.

7. The computerized method of claim 5, wherein obtaining the operating system storage key comprises:

generating a seed value; and

generating the operating system storage key based on the seed value.

8. The computerized method of claim 1, wherein the storage key comprises an application storage key and a user storage key to encrypt content containing portion specific to an application and a portion specific to a user, and obtaining the storage key comprises:

generating a seed value for the application;

producing an application hash seed value based on the seed value for the application using an application-specific one-way hash function;

generating an application storage key from the application hash seed value;

generating a seed value for the user;

producing a first user hash seed value based on the seed value for the user using a one-way hash function;

producing a second user hash seed value based on the first user hash seed value and a user identifier using a keyed hash function; and

generating a user storage key from the second user hash seed value.

9. The computerized method of claim 1, further comprising:

storing the storage key in a key vault provided by a third-party; and

recovering the storage key from the key vault.

10. The computerized method of claim 9, wherein recovering the storage key comprises:

requesting recovery of the storage key; and

providing information to the third-party to enable validation of the request.

11. The computerized method of claim 9, further comprising:

selecting the key vault from a plurality of key vaults provided by a digital rights management operating system.

12. The computerized method of claim 9, further comprising:

selecting the key vault designated by a provider of the content.

13. The computerized method of claim 1 wherein the elements are performed in the order recited.

14. A computer system comprising:

a processing unit;

a system memory coupled to the processing unit through a system bus;

a computer-readable medium coupled to the processing unit through a system bus; and

a generate key function executed from the computer-readable medium by the processing unit, wherein the generate key function causes the processing unit to generate an operating system storage key based on an identity for the operating system.

15. The computer system of claim 14, wherein the operating system storage key is further based on a seed.

16. The computer system of claim 14, further comprising:

an application specific one-way hash function executed from the computer-readable medium by the processing unit, wherein the application specific one-way hash function causes the processing unit to generate an application storage key from a hashed seed; and

a generate application key function executed from the computer-readable medium by the processing unit, wherein the generate application key function causes the processing unit to generate the hashed seed from an application seed.

17. The computer system of claim 14, further comprising:

a key-hash function executed from the computer-readable medium by the processing unit, wherein the key-hash function causes the processing unit to generate a user storage key from a hashed seed and an identity for the user;

a one-way hash function executed from the computer-readable medium by the processing unit, wherein the one-way hash function causes the processing unit to generate the hashed seed from a previously hashed seed; and

a generate user key function executed from the computer-readable medium by the processing unit, wherein the generate user key function causes the processing unit to generate the previously hashed seed from a user seed.

18. A computer system comprising:

a processing unit;

a system memory coupled to the processing unit through a system bus;

a computer-readable medium coupled to the processing unit through a system bus; and

a digital rights management operating system executed from the computer-readable medium by the processing unit, wherein the digital rights management operating system causes the processing unit to encrypt downloaded content using a storage key based on a seed value.

19. The computer system of claim 18, wherein the digital rights management operating system further causes the processing unit to encrypt an access predicate associated with the

downloaded content using an operating system storage key, to encrypt the seed value for the storage key using the operating system storage key, and to associate the encrypted access predicate with the encrypted seed value.

20. The computer system of claim 19, wherein the digital rights management operating system further causes the processing unit to validate each application requesting access to the downloaded content using the access predicate, and decrypts the seed value for use by a validated application.

21. The computer system of claim 18, wherein the storage key used to encrypt the downloaded content is specific to an application.

22. The computer system of claim 18, wherein the storage key used to encrypt the downloaded content is specific to a user.

23. A computer-readable medium having computer-executable instructions stored thereon to cause a server computer to perform a method comprising:

entering into a secure connection with a client computer;

obtaining a session key specific to the secure connection;

encrypting data with the session key; and

downloading the encrypted data to the client computer.

24. A computer-readable medium having computer-executable instructions stored thereon

to cause a client computer to perform a method comprising:

entering into a secure connection with a server computer;

obtaining a session key specific to the secure connection;

receiving data encrypted with the session key from the server computer;

storing the encrypted data on a persistent storage; and

securing the session key with a storage key.

Add C3